[8 - 2]

최적의 상관특성을 갖는 이진시퀀스군의 생성

노 종선° 건국대학교 전자공학과
정 하봉 홍익대학교 전자공학과
양 경철 한양대학교 전자통신과
송 홍엽 연세대학교 전자공학과

On the Construction of Binary Sequence Families with Optimal Correlation Properties

Jong-Seon No
Dept. of Electronic Engineering
Konkuk University

Habong Chung
Dept. of Electronic Engineering
Hong-Ik University

Kyeongcheol Yang
Dept. of Electronic Communication Engineering
Hanyang University

Hong-Yeop Song
Dept. of Electronic Engineering
Yonsei University

ABSTRACT

In this paper, we show that if there is a binary sequence with ideal autocorrelation property and it is described using the trace function, it may be used to construct a family of binary sequences with optimal correlation properties in terms of Welch's bound. In this method, the small set of Kasami sequences is interpreted as a family constructed from an m-sequence and the No sequences are interpreted as a family constructed from a decimation of the m-sequence. New optimum families of binary sequences are constructed from the Legendre sequences of Mersenne prime period using a trace representation of Legendre sequences.

I. INTRODUCTION

Code division mutiple access (CDMA) systems use pseudonoise binary sequences as signature sequences and several spread spectrum communications systems also use them as spreading codes for low probability of intercept [9]. Major characteristics which are desirable of a family of binary sequences for such applications include long period, low out-of-phase autocorrelation values, low cross-correlation values, low nontrivial partial-period correlation values, large linear span, a balance of symbols, large family size, and ease of implementation.

A binary (0 or 1) sequence $\{b(t),\ t = 0, 1, \ldots, N-1\}$ of period $N = 2^n - 1$ is called *balanced* if the number of 1's is one more than the number of 0's [3]. It is said to have the *ideal autocorrelation property* if its periodic autocorrelation function $R(\tau)$ is given by

$$R(\tau) = \begin{cases} N, & \text{for } \tau = 0 \bmod N, \\ -1, & \text{for } \tau \neq 0 \bmod N, \end{cases} \tag{1}$$

where $R(\tau)$ is defined as

$$R(\tau) = \sum_{t=0}^{N-1} (-1)^{b(t+\tau)+b(t)} \tag{2}$$

and $t+\tau$ is computed modulo N.

Consider a set of J binary sequences, each with period N, denoted by $\{v^{(j)}(t), t = 0, 1, \ldots, N-1\}$, $j = 1, 2, \ldots, J$. The periodic cross-correlation $R_{jk}(\tau)$ at shift τ between sequences from this collection is defined as

$$R_{jk}(\tau) = \sum_{t=0}^{N-1} (-1)^{v^{(j)}(t+\tau)+v^{(k)}(t)}. \tag{3}$$

The maximum out-of-phase periodic autocorrelation magnitude R_A for this signal set is defined as

$$R_A = \max_{j} \max_{0<\tau<N} |R_{jj}(\tau)|, \tag{4}$$

and the maximum cross-correlation magnitude R_C between sequences in this set is given by

$$R_C = \max_{j\neq k} \max_{0\leq\tau<N} |R_{jk}(\tau)|. \tag{5}$$

The criterion for signal design is to minimize

$$R_{\max} = \max(R_A, R_C). \tag{6}$$

In the signal design, the Welch bound and the Sidelnikov bound are used to judge the optimality for the sequence sets. Some of the well-known optimum families of these sequences include Gold sequences [1], Kasami sequences [9], bent sequences, and No sequences [5]. The small set of Kasami sequences is an optimal collection of binary sequences with respect to Welch's bound [12] which implies that

$$R_{\max} \geq 1 + 2^{n/2}, \tag{7}$$

when it is applied to a set of $2^{n/2}$ sequences of period $N = 2^n - 1$ for an even integer n. Bent sequences and No sequences also form an optimal set with respect to Welch's bound, respectively, but they have larger linear spans than Gold sequences and Kasami sequences.

In this paper, we show that if there is a binary sequence with ideal autocorrelation property and it is described using the trace function over a finite field, then there exists an explicit generalization method to construct a family of binary sequences of longer period with optimal correlation properties in terms of Welch's bound. In this method, the small set of Kasami sequences is interpreted as a family constructed from the m-sequences, and the No sequences are interpreted as a family constructed from the GMW sequences. In terms of Welch's bound, new optimum families of binary sequences are constructed from the Legendre sequences of Mersenne prime period.

This paper is organized as follows. In Section II, we present the main theorem to construct an optimal family of binary sequences from a binary sequence with ideal autocorrelation property. In Section III, the small set of Kasami sequences is interpreted as a family constructed from the m-sequences, and the No sequences are interpreted as a family constructed from the GMW sequences. As a first nontrivial example, new optimum families of binary sequences are constructed from the Legendre sequences of Mersenne prime period in Section IV.

II. Construction of a Family of Binary Sequences with Optimum Correlation

Let q be a prime power and F_q be the finite field with q elements. Let $n = em > 1$ for some positive integers e and m. Then the trace function $\mathrm{tr}_m^n(\cdot)$ is a mapping from F_{2^n} to its subfield F_{2^m} given by

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{e-1} x^{2^{mi}}.$$

In [7], No et al. present a generalization method to extend binary sequences with ideal autocorrelation property. In particular, they show that if the binary sequence $\{b(t)\}$ of period $M = 2^m - 1$ with ideal autocorrelation property is expressed using the trace function over the finite field F_2, it can be explicitly extended to a binary sequence $\{s(t)\}$ of period $N = 2^n - 1$, $m \mid n$, with ideal autocorrelation property. The idea of the extension will be helpful for the following main theorem.

Theorem 1 *Let m and n be positive integers such that $n = 2m$. Let α be a primitive element of F_{2^n} and set $\beta = \alpha^T$ where $T = 2^m + 1$. Assume that for an index set I the sequence $\{b(t_1),\ t_1 = 0, 1, \ldots, 2^m - 2\}$ given by*

$$b(t_1) = \sum_{a \in I} \mathrm{tr}_1^m(\beta^{at_1})$$

has the ideal autocorrelation property. Let $\mathcal{F}$ be the family of 2^m binary sequences of period $N = 2^n - 1$ defined by

$$\mathcal{F} = \{\{s^{(i)}(t),\ t = 0, 1, \ldots, N-1\} \mid i = 1, 2, \ldots, 2^m\}$$

where the sequence $\{s^{(i)}(t),\ t = 0, 1, \ldots, 2^n - 2\}$ is given by

$$s^{(i)}(t) = \sum_{a \in I} \mathrm{tr}_1^m\{[\mathrm{tr}_m^n(\alpha^{2t}) + \gamma_i \beta^t]^{ar}\}, \quad \text{for } \gamma_i \in F_{2^m}$$

and r, $1 \leq r \leq 2^m - 2$, is an integer relatively prime to $2^m - 1$. Then the family $\mathcal{F}$ is the optimum set of 2^m binary sequences of period N.

Proof: It suffices to show that the possible values of $R_{ij}(\tau)$ are -1, $2^m - 1$, or $-2^m - 1$ for any i, j and τ except for the case where $i = j$ and $\tau = 0 \bmod N$. Since $\gcd(2^m - 1, T) = 1$, any integer t, $0 \leq t \leq 2^{2m} - 2$, can be uniquely written as

$$t = t_1 T + t_2(2^m - 1), \quad 0 \leq t_1 \leq 2^m - 2,\ 0 \leq t_2 \leq 2^m.$$

Consider the sequence $\{s^{(i)}(t),\ t = 0, 1, \ldots, 2^n - 2\}$. Then

$$\begin{aligned} s^{(i)}(t) &= \sum_{a \in I} \mathrm{tr}_1^m\{[\mathrm{tr}_m^n(\alpha^{2t_1 T + 2t_2(2^m-1)}) + \gamma_i \beta^{t_1 T + t_2(2^m-1)}]^{ar}\} \\ &= \sum_{a \in I} \mathrm{tr}_1^m\{\beta^{2art_1}[\mathrm{tr}_m^n(\alpha^{2t_2(2^m-1)}) + \gamma_i]^{ar}\} \end{aligned}$$

since $\alpha^{2t_1 T} \in F_{2^m}$ and $\beta^T = \beta^2$. For short notation, we define

$$f(\gamma_i, t_2) = \mathrm{tr}_m^n(\alpha^{2t_2(2^m-1)}) + \gamma_i. \tag{8}$$

Then we have

$$s^{(i)}(t) = \sum_{a \in I} \mathrm{tr}_1^m\{\beta^{2art_1}[f(\gamma_i, t_2)]^{ar}\}.$$

Similarly, we have

$$s^{(j)}(t + \tau) = \sum_{a \in I} \mathrm{tr}_1^m\{\beta^{2(t_1+\tau_1)ar}[f(\gamma_j, t_2 + \tau_2)]^{ar}\}$$

where an integer τ, $0 \leq \tau \leq 2^{2m} - 2$, is also written as

$$\tau = \tau_1 T + \tau_2(2^m - 1), \quad 0 \leq \tau_1 \leq 2^m - 2,\ 0 \leq \tau_2 \leq 2^m.$$

Thus

$$
\begin{aligned}
R_{ij}(\tau) &= \sum_{t=0}^{N-1} (-1)^{s^{(i)}(t)+s^{(j)}(t+\tau)} \\
&= \sum_{t_2=0}^{2^m} \sum_{t_1=0}^{2^m-2} (-1)^{\sum_{a\in I} \mathrm{tr}_1^m \left\{\beta^{2ar t_1}\left([f(\gamma_i,t_2)]^{ar}+[\beta^{2\tau_1} f(\gamma_j,t_2+\tau_2)]^{ar}\right)\right\}}.
\end{aligned}
$$

Note that the inner sum

$$\sum_{t_1=0}^{2^m-2} (-1)^{\sum_{a\in I} \mathrm{tr}_1^m \left\{\beta^{2ar t_1}\left([f(\gamma_i,t_2)]^{ar}+[\beta^{2\tau_1} f(\gamma_j,t_2+\tau_2)]^{ar}\right)\right\}}$$

yields 2^m-1 when $f(\gamma_i,t_2)=\beta^{2\tau_1}f(\gamma_j,t_2+\tau_2)$, or -1 when $f(\gamma_i,t_2)\neq\beta^{2\tau_1}f(\gamma_j,t_2+\tau_2)$, because if either $f(\gamma_i,t_2)=0$ or $f(\gamma_j,t_2+\tau_2)=0$, the exponent to (-1) in the inner sum is essentially an shift of the sequence $\{b(t_1)\}$ and if $f(\gamma_i,t_2)\neq 0$ and $f(\gamma_j,t_2+\tau_2)\neq 0$, the inner sum is the autocorrelation of the sequence $\{b(t_1)\}$ at some shift. In order to compute $R_{ij}(\tau)$, it is necessary to estimate the size of the set of τ_2's such that the inner sum gives the value -1. Let

$$\Lambda = \{\alpha^{t_2} \mid 0 \le t_2 \le 2^m,\ \ f(\gamma_i,t_2)=\beta^{2\tau_1}f(\gamma_j,t_2+\tau_2)\}.$$

Then we have

$$
\begin{aligned}
R_{ij}(\tau) &= (2^m-1)\cdot|\Lambda| + (-1)\cdot(2^m+1-|\Lambda|) \\
&= 2^m|\Lambda| - (2^m+1).
\end{aligned}
\tag{9}
$$

By defining $x=\alpha^{2t_2(2^m-1)}$ and $u=\alpha^{2\tau_2(2^m-1)}$, we have

$$\Lambda \subset \{x\in F_{2^n} \mid x + x^{2^m} + \gamma_i = \beta^{2\tau_1}(ux + u^{2^m}x^{2^m} + \gamma_j)\}.$$

Note that $x\in F_{2^{2m}}\backslash\{0\}$ and $x^{2^{2m}}=x$, so we get

$$x^{2^m} = \alpha^{2t_2(2^m-1)\cdot 2^m} = \alpha^{-2t_2(2^m-1)} = x^{-1}.$$

Similarly, we have $u^{2m}=u^{-1}$. Thus

$$
\begin{aligned}
\Lambda &\subset \{x\in F_{2^n} \mid x + x^{-1} + \gamma_i = \beta^{2\tau_1}(ux + (ux)^{-1} + \gamma_j)\} \\
&= \{x\in F_{2^n} \mid x^2 + 1 + \gamma_i x = \beta^{2\tau_1}(ux + u^{-1} + \gamma_j x)\}.
\end{aligned}
$$

The degree of the polynomial in x is at most 2, which means $|\Lambda|\le 2$. Hence we conclude that

$$R_{ij}(\tau)\in\{-2^m-1,-1,2^m-1\}$$

from Equation (9). □

III. Kasami Sequences and No Sequences

Let m and n be positive integers such that $n=2m$. Let α be a primitive element of F_{2^n} and set $\beta=\alpha^T$ where $T=2^m+1$. Then β is a primitive element of F_{2^m}.

Let $\{b(t_1),\ t_1=0,1,\dots M-1\}$ be a binary m-sequence of period $M=2^m-1$. Then it is well-known that $\{b(t_1)\}$ can be expressed as

$$b(t_1) = \mathrm{tr}_1^m(\beta^{t_1}). \tag{10}$$

Note that the m-sequence $\{b(t_1)\}$ is a binary sequence with ideal autocorrelation property. Applying theorem 1 to $\{b(t_1)\}$, we can get an optimal family $\mathcal{F}$ defined by

$$\mathcal{F} = \{\{s^{(i)}(t),\ t=0,1,\dots,N-1\} \mid i=1,2,\dots,2^m\}$$

where $\{s^{(i)}(t),\ t=0,1,\dots,2^n-2\}$ be the sequence given by

$$s^{(i)}(t) = \mathrm{tr}_1^m\{[\mathrm{tr}_m^n(\alpha^{2t})+\gamma_i\beta^t]^r\}$$

for $\gamma_i\in F_{2^m}$. Note that the family $\mathcal{F}$ is exactly the family of No sequences [5]. In particular, the family $\mathcal{F}$ is the small set of Kasami sequences when $r=1$ [6]. Hence Theorem 1 provides a generalization method to construct a family of binary sequences with optimum correlation.

IV. New Families of Binary Sequences Constructed from Legendre Sequences

Let p be an odd prime. The Legendre sequences $\{b(t),\ t=0,1,\dots p-1\}$ of period p is defined as

$$
b(t) = \begin{cases} 1 & \text{if } t=0 \mod p, \\ 0 & \text{if } t \text{ is a quadratic residue mod } p, \\ 1 & \text{if } t \text{ is a quadratic non-residue mod } p. \end{cases}
\tag{11}
$$

It is not difficult to show that $\{b(t)\}$ has the ideal autocorrelation property if and only if $p=3 \pmod 4$ [4].

It seems to be quite difficult to find any simple and explicit representation of the Legendre sequence $\{b(t)\}$ for all primes $p=3 \pmod 4$ using the trace function over a finite field. However, it is recently shown that the Legendre sequences of period $p=2^m-1$ can be explicitly described using the trace function from the finite field with 2^m elements to the binary field [8].

Proposition 2 *Let $p=2^m-1$ be a prime for some integer $m\ge 3$ and u be a primitive element of Z_p, the set of intgers mod p. Then there exists a primitive element β of F_{2^m} such that*

$$\sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m(\beta^{u^{2j}}) = 0, \tag{12}$$

and the sequence $\{s(t),\ \ t=0,1,2,\dots,p-1\}$ of period p given by

$$s(t) = \sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^n(\beta^{u^{2j}t}) \tag{13}$$

is exactly the Legendre sequence given in Eq.(11).

The following theorem are the consequences of main theorem in [7] and theorem 1.

Theorem 3 *Let m be an integer such that $p=2^m-1$ is prime and let $n=2m$. Let u be a primitive element of Z_p, the set of intgers mod p. Let α be a primitive element of*

F_{2^n} and set $\beta = \alpha^T$ where $T = 2^m + 1$. Let $\{s^{(i)}(t),\ t = 0, 1, \ldots, N-1\}$ be the sequence of period $N = 2^n - 1$ given by

$$s^{(i)}(t) = \sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m\{[\mathrm{tr}_m^n(\alpha^{2t}) + \gamma_i\beta^t]^{u^{2j}r}\}, \quad \textit{for}\ \ \gamma_i \in F_{2^m}$$

and r, $1 \leq r \leq 2^m - 2$, is an integer relatively prime to $2^m - 1$. Then the family $\mathcal{F}$ defined by

$$\mathcal{F} = \{\{s^{(i)}(t),\ t = 0, 1, \ldots, N-1\} \mid i = 1, 2, \ldots, 2^m\}$$

is the optimum set of 2^m binary sequences of period $N = 2^n - 1$.

Example 4 Let $m = 7$ and thus $p = 127 (= 2^7 - 1)$. It is easy to check that $u = 3$ is a primitive element in Z_{127}. Let β be the primitive element of F_{2^7} satisfying $\beta^7 + \beta^4 + 1 = 0$. Then we have

$$\sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m(\beta^{u^{2j}}) = \sum_{j=0}^{8} \mathrm{tr}_1^7(\beta^{3^{2j}}) = 0.$$

The sequence $\{b(t_1),\ t_1 = 0, 1, \ldots, 126\}$ given by

$$b(t_1) = \sum_{j=0}^{8} \mathrm{tr}_1^7(\beta^{3^{2j}t_1}) = \sum_{j=0}^{8} \mathrm{tr}_1^7(\beta^{9^j t_1})$$

is the Legendre sequence of period 127.

Let n be a multiple of $m = 7$. Let α be a primitive element of F_{2^n} and set $T = (2^n - 1)/(2^m - 1)$. Then the sequence $\{b(t_1)\}$ can be extended to a binary sequence of period $2^n - 1$ with ideal autocorrelation property. That is, the sequence $\{s(t),\ \ t = 0, 1, \cdots, 2^n - 2\}$ of period $N = 2^n - 1$ given by

$$s(t) = \sum_{j=0}^{8} \mathrm{tr}_1^7\{[\mathrm{tr}_7^n(\alpha^t)]^{u^{2j}r}\}$$

has the ideal autocorrelation property.

Now we restrict n in the case that $n = 2m = 14$. Define

$$s^{(i)}(t) = \sum_{j=0}^{8} \mathrm{tr}_1^7\{[\mathrm{tr}_7^{14}(\alpha^{2t}) + \gamma_i\beta^t]^{u^{2j}r}\}, \quad \text{for}\ \ \gamma_i \in F_{2^7}.$$

Then the family $\mathcal{F}$ defined by

$$\mathcal{F} = \{\{s^{(i)}(t),\ t = 0, 1, \ldots, N-1\} \mid i = 1, 2, \ldots, 2^m\}$$

is the optimum set of 128 binary sequences of period $N = 2^{14} - 1$ with respect to Welch's bound.

References

[1] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619-621, Oct. 1967.

[2] S. W. Golomb, "On the classification of balanced binary sequences of period $2^n - 1$," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 730-732, Nov. 1980.

[3] S. W. Golomb, *Shift-Register Sequences*, Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA 1982.

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[5] J. -S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. IT-35, pp. 371-379, Mar. 1989.

[6] J. -S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory*, vol. IT-42, pp. 260-262, Jan. 1996.

[7] J. -S. No, H. Chung, K. Yang and H. -Y. Song, "Extension of binary sequences with ideal autocorrelation property," preprint, Mar. 1996.

[8] J. -S. No, H. -K. Lee, H. Chung, H. -Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," preprint, Feb. 1996.

[9] D. V. Sarwate and M. B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences," *Proc. IEEE*, vol. IT-68, pp. 593-619, May 1980.

[10] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548-553, May 1984.

[11] H. Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference sets," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1266-1268, July 1994.

[12] L. R. Welch, "Lower bounds on the maximum cross-correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397-399, May 1994.